UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MISSOURI

IN RE: PANERA DATA SECURITY LITIGATION	Master File No. 4:24-cv-00847
This Document Relates To: All Actions	**AMENDED CONSOLIDATED CLASS ACTION COMPLAINT**
	JURY TRIAL DEMANDED

Plaintiffs Samantha Baldwin, Matthew Baldwin, Thomas Jones, Messiah Jordan Weddle, Gracelyn Donovan, Sydney Hollis, Robyn Campbell, Amanda Pharr, Forrest Cooley and Taslima Aktar ("Plaintiffs"), individually and on behalf of all other similarly situated individuals (the "Class" or "Class Members" as defined below) and by and through their undersigned counsel, file this Amended Consolidated Class Action Complaint against Defendant Panera, LLC ("Panera" or "Defendant") and allege the following based upon personal knowledge of facts pertaining to themselves and upon information and belief based upon the investigation of counsel as to all other matters.

NATURE OF THE ACTION

1. With this action, Plaintiffs seek to hold Defendant responsible for the harms it caused them and the other Class Members in the large and preventable data breach that was discovered by Panera on March 23, 2024, and announced publicly by Panera on June 13, 2024, in which unauthorized users accessed Panera servers that contained personal information of current and former employees and business partners ("Data Breach" or "Breach").[1]

2. Every year millions of Americans have their most valuable personal identifying

[1] State of California Department of Justice, *Panera Bread Notice of Data Breach*, https://oag.ca.gov/system/files/Panera_CA%20App%20%26%20Sample_0.pdf (last visited January 21, 2025).

information stolen and sold online because of preventable data breaches. Despite the dire warnings about the severe impact of data breaches on Americans of all economic strata, some businesses still fail to put adequate security measures in place to protect their customers' and employees' data.

3. Defendant Panera, an American chain store of bakery-café restaurants, is renowned for providing a diverse menu that includes pastries, coffee, pizzas, salads, pasta, and more. With sales amounting to $6.34 billion in 2022, Defendant is ranked as the second-largest bakery café chain in the United States.[2]

4. The Data Breach itself occurred on February 9, 2024, during which an unauthorized third party targeted and gained access to Defendant's internal files that contained sensitive employees' data.[3] However, it took Defendant until March 23, 2024, to finally discover it, over a month later.[4] Although Defendant has not yet disclosed the total number of individuals affected, its investigation confirmed on May 16, 2024, that those files compromised contain employees' Personally Identifiable Information ("PII"), including but not limited to, full names and Social Security numbers.[5] On or around June 13, 2024, Defendant began sending letters ("Notice Letters") to affected individuals notifying them that their information was compromised. According to the Notice Letter, other information that Defendant collected from affected

---

[2] Statista, *Leading Bakery Cafe Chains in the United States in 2022, by Systemwide Sales*, https://www.statista.com/statistics/1115824/bakery-cafe-chains-highest-sales-us/ (last visited Jan. 14, 2025)
[3] Defendant's report to the Office of the Maine Attorney General: https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/9366354d-de2c-468a-9e81-7fece7463aeb.html (last visited Jan. 14, 2025).
[4] State of California Department of Justice, *Panera Bread Notice of Data Breach*, https://oag.ca.gov/system/files/Panera_CA%20App%20%26%20Sample_0.pdf (last visited January 21, 2025).
[5] *Id.*

individuals upon their employment might also have been impacted.[6] However, no additional details have been announced yet.

5. As a condition of employment, Plaintiffs and the Class Members were required to disclose their PII to Defendant, entrusting Defendant with keeping it safe and protected.

6. As a corporation doing business in multiple states through the U.S., Defendant is legally required to protect the PII it gathers from unauthorized access and exfiltration. Given Defendant's sophistication as a well-known business, it knows and should have known its legal obligation to safeguard its cybersecurity.

7. The Data Breach was the result of Defendant's failure in establishing, implementing, and maintaining reasonable policies and adequate procedures to safeguard the PII it collected as part of its business. This unencrypted PII was compromised due to Defendant's negligent and/or careless actions and its complete failure to protect the PII of its users. Hackers targeted and acquired the PII of Plaintiffs and Class Members because of its value in exploiting and stealing the identities of Plaintiffs and Class Members.

8. Given the particularly sensitive nature of the exposed data, Plaintiffs and Class Members have suffered irreparable harm and are subject to an increased risk of identity theft for the foreseeable future.

THE PARTIES

9. Defendant Panera is an American chain store of bakery-café restaurants headquartered in St. Louis, MO.

10. Plaintiff Samantha Baldwin is an adult individual, who is a resident and citizen of North Carolina, where she intends to stay.

---

[6] *Id*.

11. Plaintiff Matthew Baldwin is an adult individual, who is a resident and citizen of North Carolina, where she intends to stay.

12. Plaintiff Thomas Jones is an adult individual, who is was a resident and citizen of Arizona, where he intends to stay.

13. Plaintiff Messiah Jordan Weddle is an adult individual, who is a resident and citizen of California, where she intends to stay.

14. Plaintiff Gracelyn Donovan is an adult individual, who is a resident and citizen of New Jersey, where she intends to stay.

15. Plaintiff Sydney Hollis is an adult individual, who is a resident and citizen of Illinois, where she intends to stay.

16. Plaintiff Robyn Campbell is an adult individual, who is a resident and citizen of Texas, where she intends to stay.

17. Plaintiff Amanda Pharr is an adult individual, who is a resident and citizen of Indiana, where she intends to stay.

18. Plaintiff Forrest Cooley is an adult individual, who is a resident and citizen of Kentucky, where he intends to stay.

19. Plaintiff Taslima Aktar is an adult individual, who is a resident and citizen of Missouri, where she intends to stay.

20. Plaintiffs reasonably believed Defendant would keep their PII secure. Had Defendant disclosed to Plaintiffs that their PII would not be kept secure and would be easily accessible to hackers and third parties, they would not have provided it to Defendant.

21. Plaintiffs each received a notice letter from Defendant, dated on or around June 13, 2024, informing them of the Data Breach and that their name, Social Security numbers, and

potentially other information provided by them were all compromised in the Data Breach.

JURISDICTION AND VENUE

22. Subject matter jurisdiction in this civil action is authorized pursuant to 28 U.S.C. § 1332(d) because there are more than 100 Class Members, at least one Class member is a citizen of a state different from that of Defendant, and the amount in controversy exceeds $5 million, exclusive of interest and costs.

23. This Court has personal jurisdiction over Defendant because it maintains its principal place of business in this District, is registered to conduct business in Missouri, and has sufficient minimum contacts with Missouri.

24. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because Defendant resides in this District and a substantial part of the events or omissions giving rise to Plaintiffs' and Class Members' claims occurred in this District.

25. Application of Missouri law to this dispute is proper because Defendant's headquarters are in Missouri, the decisions or actions that gave rise to the underlying facts at issue in this Complaint were presumably made or taken in Missouri, and the action and/or inaction at issue emanated from Missouri.

FACTUAL ALLEGATIONS

A. Defendant collects and stores thousands of current and former employees' PII and fails to provide adequate data security.

26. Founded in 1987, Defendant Panera, LLC, is an American chain store of bakery-café restaurants headquartered in St. Louis, MO. With over 2,000 locations throughout the United States and Canada, Defendant has approximately 14,000 employees as of 2023.

27. Plaintiffs and Class Members relied on this sophisticated Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and

to make only authorized disclosures of this information. Plaintiffs and Class Members demand security to safeguard their sensitive PII.

28. Defendant had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' PII from disclosure to third parties. However, Defendant failed to fulfill this duty.

B. Panera's inadequate data security exposes its employees' sensitive PII.

29. On or about February 9, 2024, unknown third-party cyber criminals gained access to Defendant's system that stores employees' data. PII including at least employees' names and SSNs have been accessed and acquired by the hackers.

30. Beginning on June 13, 2024, Plaintiffs received letters from Panera ("Notice Letter"), notifying them that their PII, including at least their full names and SSNs, may have been compromised. Specifically, the Notice Letter states the following:

> Panera, LLC ("Panera") is writing to notify you of a security incident that involved some of your information. We understand the importance of protecting the information we maintain, and this letter explains what happened, the measures we have taken, and steps you may consider taking.
>
> Panera detected and took measures to address the incident on March 23, 2024. A cybersecurity firm was engaged. A thorough investigation identified unauthorized access to internal files occurring that day. We also notified law enforcement. The files involved were reviewed, and on May 16, 2024, we determined that a file contained your name and Social Security number. Other information you provided in connection with your employment could have been in the files involved. As of the date of mailing of this letter, there is no indication that the information accessed has been made publicly available.

C. The Compromised PII is valuable.

31. When malicious actors infiltrate companies and copy and exfiltrate the PII that those companies store, the stolen information often ends up on the dark web because the

malicious actors buy and sell the information for profit.[7]

32. "Ransomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for complaints as revenge against those who refuse to pay."[8]

33. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[9]

34. Stolen PII is often trafficked on the dark web, as is the case here. Law enforcement has difficulty policing the dark web due to encryption, which allows users and criminals to conceal identities and online activity.

35. Another example is when the U.S. Department of Justice announced its seizure of AlphaBay in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity. Other marketplaces, similar to the now-defunct AlphaBay, "are awash with [PII] belonging to victims from countries all over the world. One of the key challenges of protecting PII online is its

---

[7] *Shining a Light on the Dark Web with Identity Monitoring,* IDENTITYFORCE (updated Feb. 1, 2020), https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited Jan. 14, 2025).

[8] Catalin Cimpanu, *Ransomware mentioned in 1,000+ SEC filings over the past year*, ZDNET (April 30, 2020), https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/(last visited Jan. 14, 2025).

[9] *See Ransomware Guide*, Multi-State Information Sharing & Analysis Center (Sept. 2020), https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf. (last visited Jan. 14, 2025).

pervasiveness. As data breaches in the news continue to show, PII about employees, customers and the public is housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[10]

36. The PII of consumers is of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at prices ranging from $40 to $200, and bank details have a price range of $50 to $200.[11] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[12]

37. Social Security numbers are among the worst kinds of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[13]

---

[10] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, ARMOR CLOUD SECURITY (April 3, 2018), https://res.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/(last visited Jan. 14, 2025).
[11] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs*, DIGITAL TRENDS (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/(last visited Jan. 14, 2025).
[12] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/(last visited Jan. 14, 2025).
[13] *Identity Theft and Your Social Security Number*, SOCIAL SECURITY ADMINISTRATION,

38. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

39. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[14]

40. Because of this, the information compromised in the Data Breach here is significantly more harmful to lose than other types of data because the information compromised in this Data Breach is difficult, if not impossible, to change.

41. The PII compromised in the Data Breach also demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained: "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10 times on the black market."[15]

42. Once PII is sold, it is often used to gain access to various areas of the victim's

---

https://www.ssa.gov/pubs/EN-05-10064.pdf#:~:text=Identity%20theft%20is%20one%20of%20the%20fastest%20growing,to%20apply%20for%20more%20credit%20in%20your%20name (last visited Jan. 14, 2025).

[14] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen- by-anthem-s-hackers-has-millions-worrying- about-identity-theft (last visited Jan. 14, 2025).

[15] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, REDSEAL, (Feb. 6, 2015), https://www.redseal.net/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers/(last visited Jan. 14, 2025).

digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional PII being harvested from the victim, as well as PII from family, friends, and colleagues of the original victim.

43. An active, robust, and legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion.[16]

44. According to the FBI's Internet Crime Complaint Center (IC3) 2023 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2023, resulting in more than $12.5 billion in losses to individuals and business victims, a twenty-two (22) percent increase in losses suffered compared to 2022.[17]

45. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

46. Data breaches facilitate identity theft as hackers obtain consumers' PII and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PII to others who do the same.

47. For example, the United States Government Accountability Office noted in a June 2007 report on data breaches (the "GAO Report") that criminals use PII to open financial accounts, receive government benefits, and make purchases and secure credit in a victim's

---

[16] David Lazarus, *Shadowy data brokers make the most of their invisibility cloak*, LA TIMES (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited Jan. 14, 2025).

[17] *See* Federal Bureau of Investigation Internet Crime Report 2023, INTERNET CRIME COMPLAINT CENTER, *available at* https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf?trk=public_post_comment-text (last visited Jan. 14, 2025).

name.[18] The GAO Report further notes that this type of identity fraud is the most harmful because it may take some time for a victim to become aware of the fraud, and can adversely impact the victim's credit rating in the meantime. The GAO Report also states that identity theft victims will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."[19]

48. The exposure of Plaintiffs' and Class Members' PII to cybercriminals will continue to cause substantial risk of future harm (including identity theft) that is continuing and imminent in light of the many different avenues of fraud and identity theft utilized by third-party cybercriminals to profit off of this highly sensitive information.

D. Panera failed to comply with Federal Trade Commission requirements.

49. The FTC has issued several guidance documents for businesses, highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be considered for all business decision-making.[20]

50. The FTC notes that businesses should safeguard the personal customer information they retain; properly dispose of unnecessary personal information; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to rectify security issues.[21]

---

[18] *See Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown*, U.S. GOVERNMENT ACCOUNTABILITY OFFICE (June 5, 2007), https://www.gao.gov/products/gao-07-737 (last visited Jan. 14, 2025).
[19] *Id.*
[20] *Start With Security: A Guide for Businesses (Lessons Learned from FTC Cases)*, FED. TRADE COMM'N ("FTC") (June 2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Jan. 14, 2025)
[21] *Protecting Personal Information: A Guide for Business*, FTC (Oct. 2016), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Jan. 14, 2025).

51. The FTC guidelines also suggest that businesses use an intrusion detection system to expose a breach as soon as it happens, monitor all incoming traffic for activity indicating someone is trying to hack the system, watch for large amounts of data being siphoned from the system, and have a response plan in the event of a breach.

52. The FTC advises companies to not keep information for periods of time longer than needed to authorize a transaction, restrict access to private information, mandate complex passwords to be used on networks, utilize industry-standard methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[22]

53. The FTC has brought enforcement actions against companies for failing to adequately and reasonably protect consumer data, treating the failure to do so as an unfair act or practice barred by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders originating from these actions further elucidate the measures businesses must take to satisfy their data security obligations.

54. Defendant Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

55. Plaintiffs and Class Members gave their PII to Defendant with the reasonable expectation and understanding that Defendant would comply with its duty to keep such information confidential and secure from unauthorized access.

---

[22] *Start With Security: A Guide for Businesses (Lessons Learned from FTC Cases)*, FED. TRADE COMM'N ("FTC") (June 2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Jan. 14, 2025).

56. Defendant has been on notice for years that Plaintiffs' and Class Members' PII was a target for bad actors because, among other motives, the high value of the PII created, collected, stored, and maintained by Defendant.

57. Despite such awareness, Defendant failed to impose and maintain reasonable and appropriate data security controls to protect Plaintiffs' and Class Members' PII from unauthorized access that Defendant should have anticipated and guarded against.

58. Defendant was fully aware of its obligation to protect the PII of its employees because of its collection, storage, and maintenance of PII. Defendant was also aware of the significant consequences that would ensue if it failed to do so because it collected, stored, and maintained sensitive private information from millions of individuals and knew that this information, if hacked, would result in injury to Plaintiffs and Class Members.

59. Despite understanding the consequences of insufficient data security, Defendant failed to adequately protect Plaintiffs' and Class Members' PII, permitting bad actors to access and misuse it.

E. Defendant failed to comply with industry standards.

60. Various cybersecurity industry best practices have been published and should be consulted as a go-to resource when developing an organization's cybersecurity standards. The Center for Internet Security ("CIS") promulgated its Critical Security Controls, which identify the most commonplace and essential cyber-attacks that affect businesses every day and proposes solutions to defend against those cyber-attacks.[23] All organizations collecting and handling PII, such as Defendant, are strongly encouraged to follow these controls.

---

[23] *Critical Security Controls*, CENTER FOR INTERNET SECURITY (May 2021), *available at* https://learn.cisecurity.org/CIS-Controls-v8-guide-pdf (last visited Jan.14, 2025).

61. Further, the CIS Benchmarks are the overwhelming option of choice for auditors worldwide when advising organizations on the adoption of a secure build standard for any governance and security initiative, including PCI DSS, HIPAA, NIST 800-53, SOX, FISMA, ISO/IEC 27002, and ITIL.[24]

62. Cybersecurity experts normally identified companies like Defendant as being particularly vulnerable to cyberattacks because of the value of the PII which they collect, use, and maintain.[25]

63. Several best practices have been identified that a minimum should be implemented by data management companies like Defendant, including but not limited to securely configuring business software, managing access controls and vulnerabilities to networks, systems, and software, maintaining network infrastructure, defending networks, adopting data encryption while data is both in transit and at rest, and securing application software.[26]

64. Defendant failed to follow these and other industry standards to adequately protect the Private Information of Plaintiffs and Class Members.

---

[24] *See CIS Benchmarks FAQ*, CENTER FOR INTERNET SECURITY, https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq/ (last visited Jan.14, 2025).

[25] *See* Joao-Pierre S. Ruth, *Security Questions to Ask After the Zeroed-In Breach*, INFORMATION WEEK (Dec. 5, 2023), https://www.informationweek.com/cyber-resilience/security-questions-to-ask-after-the-zeroedin-breach (commenting that the growing outsourcing of data analytics work to third-party service providers may offer to malicious cyber-attackers novel "targets of opportunity" – breach one data manager and gain access to data from a multitude of sources) (last visited Jan.14, 20254).

[26] *See Critical Security Controls*, CENTER FOR INTERNET SECURITY (May 2021), *available at* https://learn.cisecurity.org/CIS-Controls-v8-guide-pdf (last visited Jan.14, 2025).

F. The Data Breach caused harm and will result in additional fraud.

65. Without detailed disclosure to the victims of the Data Breach, individuals whose Private Information was compromised by the Data Breach, including Plaintiffs and Class Members, were unknowingly and unwittingly exposed to continued misuse and ongoing risk of misuse of their Private Information for months without being able to take available precautions to prevent imminent harm.

66. The ramifications of Defendant's failure to secure Plaintiffs' and Class Members' data are severe.

67. Victims of data breaches are much more likely to become victims of identity theft and other types of fraudulent schemes. This conclusion is based on an analysis of four years of data that correlated each year's data breach victims with those who also reported being victims of identity fraud.

68. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[27] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[28]

69. Identity thieves can use PII, such as that of Plaintiffs and Class Members, which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture;

[27] 17 C.F.R § 248.201 (2013).
[28] *Id.*

using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

70. As demonstrated herein, these and other instances of fraudulent misuse of the compromised PII have already occurred and are likely to continue.

71. As a result of Defendant's delay between the Data Breach in February 2024 and the notice of the Data Breach sent to affected persons in June 2024, the risk of fraud for Plaintiffs and Class Members increased exponentially.

72. Javelin Strategy and Research reports that identity thieves have stolen $112 billion in the past six years.[29]

73. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[30]

74. There may be a time lag between when harm occurs versus when it is discovered, and also between when private information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting

---

[29] *See* https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point (last visited Jan. 14, 2025).

[30] *Victims of Identity Theft*, Bureau of Justice Statistics (Sept. 2015) available at: https://bjs.ojp.gov/library/publications/victims-identity-theft-2014 (last visited Jan. 14, 2025).

from data breaches cannot necessarily rule out all future harm.[31]

75. Thus, Plaintiffs and Class Members now constant surveillance of their financial and personal records, monitoring, and loss of rights, for the foreseeable future.

G. Plaintiffs and Class Members suffered damages.

76. The Data Breach was a direct and proximate result of Defendant's failure to properly safeguard and protect Plaintiffs' and Class Members' Private Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law, including but not limited to, Defendant's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class Members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

77. Had Defendant remedied the deficiencies in their information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, they would have prevented intrusion into its information storage and security systems.

78. As a direct and proximate result of Defendant's wrongful actions and inaction and the resulting Data Breach, Plaintiffs and Class Members have already been harmed by the fraudulent misuse of their PII, and have been placed at an imminent, immediate, and continuing increased risk of additional harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate both the actual and potential impact of the Data Breach on their

[31] GAO, *Report to Congressional Requesters*, at 29 (June 2007), *available at* http://www.gao.gov/new.items/d07737.pdf (last visited Jan. 18, 2024).

lives. Such mitigatory actions include, inter alia, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, sorting through dozens of phishing and spam email, text, and phone communications, and filing police reports. This time has been lost forever and cannot be recaptured.

79. Defendant's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and Class Members' PII, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft and misuse of their personal and financial information;

b. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals and misused via the sale of Plaintiffs' and Class Members' information on the Internet's black market;

c. the untimely and inadequate notification of the Data Breach;

d. the improper disclosure of their PII;

e. loss of privacy;

f. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

g. ascertainable losses in the form of deprivation of the value of their PII, for which there is a well-established national and international market; and,

h. the loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data

Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the inconvenience, nuisance and annoyance of dealing with all such issues resulting from the Data Breach.

80. While Plaintiffs' and Class Members' PII has been stolen, Defendant continues to hold Plaintiffs' and Class Members' PII. Particularly because Defendant has demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiffs and Class Members have an undeniable interest in ensuring that their PII is secure, remains secure, is properly and promptly destroyed, and is not subject to further theft.

H. Panera's delay in identifying and reporting the breach caused additional harm.

81. While the initial Data Breach occurred on February 9, 2024, affected current and former employees were not notified of the Data Breach until June 13, 2024, or later and are unaware of how long their PII has been exposed to cyber criminals, thus depriving them of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach.

82. As a result of Panera's potential delay in detecting and notifying the affected individuals of the Data Breach, the risk of fraud for Plaintiffs and Class Members has been driven even higher.

PLAINTIFFS' EXPERIENCE

Plaintiff Samantha Baldwin

83. Plaintiff Samantha Baldwin, who was employed by Defendant at the time of the Data Breach, received Defendant's Notice of Data Breach, dated June 13, 2024, on or about that date. The notice stated that her name and Social Security number were impacted.

84. As a result of the Data Breach, Plaintiff Samantha Baldwin's sensitive information was accessed and/or acquired by an unauthorized actor. The confidentiality of Plaintiff Samantha Baldwin's sensitive information has been irreparably harmed. For the rest of her life, Plaintiff Samantha Baldwin will have to worry about when and how her sensitive information may be shared or used to her detriment.

85. As a result of the Data Breach notice, Plaintiff Samantha Baldwin spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

86. Additionally, Plaintiff Samantha Baldwin is very careful about sharing her sensitive PII. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

87. Plaintiff Samantha Baldwin stores any documents containing her sensitive PII in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

88. Plaintiff Samantha Baldwin suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

89. Plaintiff Samantha Baldwin has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially her Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

90. Plaintiff Samantha Baldwin has a continuing interest in ensuring that her PII,

which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Matthew Baldwin

91. Plaintiff Matthew Baldwin, who was employed by Defendant at the time of the Data Breach, received Defendant's Notice of Data Breach, dated June 13, 2024, on or about that date. The notice stated that his name and Social Security number were impacted.

92. As a result of the Data Breach, Plaintiff Matthew Baldwin's sensitive information was accessed and/or acquired by an unauthorized actor. The confidentiality of Plaintiff Matthew Baldwin's sensitive information has been irreparably harmed. For the rest of his life, Plaintiff Matthew Baldwin will have to worry about when and how his sensitive information may be shared or used to his detriment.

93. As a result of the Data Breach notice, Plaintiff Matthew Baldwin spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

94. Additionally, Plaintiff Matthew Baldwin is very careful about sharing his sensitive PII. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

95. Plaintiff Matthew Baldwin stores any documents containing his sensitive PII in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

96. Plaintiff Matthew Baldwin suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss

of his privacy.

97. Plaintiff Matthew Baldwin has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

98. Plaintiff Matthew Baldwin has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Thomas Jones

99. Plaintiff Thomas Jones is a resident of Gilbert, Arizona.

100. Plaintiff Jones is employed by Defendant and has been since March 2023. As a condition of his employment, Plaintiff Jones was required to provide Defendant with his full name, date of birth, address, bank account information, birth certificate, and Social Security number.

101. Plaintiff Jones values his privacy and makes every effort to keep his personal information private.

102. Plaintiff Jones only allowed Defendant to maintain, store, and use his Private Information because he believed Defendant would use basic security measures to protect his PII, such as requiring passwords and multi-factor authentication to access databases storing his Private Information.

103. In the instant that his PII was accessed and obtained by a third party without his consent or authorization, Plaintiff Jones suffered injury from a loss of privacy.

104. Plaintiff Jones has been further injured by the damages to and diminution in value

of his PII—a form of intangible property that Plaintiff Jones entrusted to Defendant. This information has inherent value that Plaintiff Jones was deprived of when his PII was placed on a publicly accessible database, exfiltrated by cybercriminals.

105. After the Data Breach occurred, Plaintiff Jones experienced a significant increase in spam calls and phishing emails.

106. Plaintiff Jones has experienced fraud and identity theft as a result of the Data Breach including having a fraudulent tax return filed in his name causing him to stop receiving his monthly Social Security payments, to which he is legally entitled, as the fraudulent tax return made it appear as if he had a higher income than he actually did, which caused him to no longer qualify for the benefits in question.

107. Plaintiff Jones expended substantial time and effort correcting the situation, involving substantial travel, including to his local congressperson's district office and three separate trips to the Social Security Administration's offices. Plaintiff Jones also had to spend time on the telephone with the Internal Revenue Service to try to correct the tax fraud he had experienced and start receiving his benefits again, and also to lock his credit and contact the credit bureaus.

108. Plaintiff Jones believes that the fraud he experienced was due to the Data Breach because it occurred shortly after the Data Breach happened and because had never previously been involved in a data breach to his knowledge.

109. The Data Breach has also caused Plaintiff Jones to suffer imminent and impending injury arising from the present and substantially increased risk of future fraud, identity theft, and misuse resulting from his PII being placed in the hands of criminals.

110. As a result of the actual harm, Plaintiff Jones has suffered the present and

increased imminent risk of future harm, including lost time spent researching the data breach and monitoring his credit and bank accounts.

111. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Jones to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, reviewing financial statements, and monitoring potential fraudulent activities. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

112. The present and substantial risk of imminent harm and loss of privacy have caused Plaintiff Jones to suffer stress, fear, and anxiety.

113. Plaintiff Jones has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Messiah Jordan Weddle

114. Plaintiff Messiah Jordan Weddle is a resident of Bakersfield, California.

115. Plaintiff Weddle was employed by Defendant in 2022. As a condition of her employment, Plaintiff Weddle was required to provide Defendant with her full name, date of birth, address, bank account information, birth certificate, and Social Security number.

116. Plaintiff Weddle values her privacy and makes every effort to keep her personal information private.

117. Plaintiff Weddle only allowed Defendant to maintain, store, and use her Private Information because she believed Defendant would use basic security measures to protect her PII, such as requiring passwords and multi-factor authentication to access databases storing her Private Information.

118. In the instant that her PII was accessed and obtained by a third party without her consent or authorization, Plaintiff Weddle suffered injury from a loss of privacy.

119. Plaintiff Weddle has been further injured by the damages to and diminution in value of her PII—a form of intangible property that Plaintiff Weddle entrusted to Defendant. This information has inherent value that Plaintiff Weddle was deprived of when her PII was placed on a publicly accessible database, exfiltrated by cybercriminals.

120. After the Data Breach occurred, Plaintiff Weddle has experienced a significant increase in spam calls and phishing emails.

121. As a result of the Data Breach, Plaintiff Weddle has suffered actual fraud and identity theft in that an unauthorized third-party attempted to take out student loans in her name.

122. Furthermore, after the Data Breach occurred, Plaintiff Weddle received an invoice for two hospital visits to Dignity Health Hospital in Utah despite never having traveled to Utah and never having been a patient at Dignity Health Hospital.

123. Plaintiff Weddle believes the above fraud is a result of the data breach because both incidents happened after the Data Breach and because she has been notified by Credit Karma that her Personal Information has been posted on the Dark Web.

124. Plaintiff Weddle has experienced direct out-of-pocket losses as a result of the data breach including the cost of postage to send letters to Dignity Health Hospital to address the fraudulent invoice and also has continuing expenses paying for credit monitoring and identity theft protection through Experian for $25 per month.

125. The Data Breach has also caused Plaintiff Weddle to suffer imminent and impending injury arising from the present and substantially increased risk of future fraud, identity theft, and misuse resulting from her PII being placed in the hands of criminals.

126. As a result of the actual harm, Plaintiff Weddle has suffered the present and increased imminent risk of future harm, including lost time spent researching the data breach and monitoring her credit and bank accounts.

127. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Weddle to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, reviewing financial statements, and signing up for credit monitoring service and monitoring potential fraudulent activities. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

128. The present and substantial risk of imminent harm and loss of privacy have caused Plaintiff Weddle to suffer stress, fear, and anxiety.

129. Plaintiff Weddle has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Gracelyn Donovan

130. Plaintiff Gracelyn Donovan is a resident of Columbia, New Jersey.

131. Plaintiff Donovan is a former employee of Defendant. As a condition of her employment, Plaintiff Donovan was required to provide Defendant with her full name, date of birth, address, bank account information, birth certificate, and Social Security number.

132. Plaintiff Donovan values her privacy and makes every effort to keep her personal information private.

133. Plaintiff Donovan only allowed Defendant to maintain, store, and use her Private Information because she believed Defendant would use basic security measures to protect her

PII, such as requiring passwords and multi-factor authentication to access databases storing her Private Information.

134. In fact, when Defendant required Plaintiff Donovan to install an "app" onto her personal telephone to track her working times, Plaintiff Donovan immediately received a notification that all of her passwords which had been saved in her telephone were "leaked" to this app. Upon receiving this notification Plaintiff Donovan refused to use the "app" in question and was terminated as a result of her concerns over protecting her Private Information.

135. In the instant that her PII was accessed and obtained by a third party without her consent or authorization, Plaintiff Donovan suffered injury from a loss of privacy.

136. Plaintiff Donovan has been further injured by the damages to and diminution in value of her PII—a form of intangible property that Plaintiff Donovan entrusted to Defendant. This information has inherent value that Plaintiff Donovan was deprived of when her PII was placed on a publicly accessible database, exfiltrated by cybercriminals.

137. After the Data Breach occurred, Plaintiff Donovan experienced a significant increase in spam calls and phishing emails.

138. The Data Breach has also caused Plaintiff Donovan to suffer imminent and impending injury arising from the present and substantially increased risk of future fraud, identity theft, and misuse resulting from her PII being placed in the hands of criminals.

139. As a result of the actual harm, Plaintiff Donovan has suffered the present and increased imminent risk of future harm, including lost time spent researching the data breach and monitoring her credit and bank accounts, including freezing her credit and changing the passwords on all of her accounts.

140. In addition to the increased risk and the actual harm suffered, the Data Breach has

caused Plaintiff Donovan to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, reviewing financial statements, and monitoring potential fraudulent activities. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

141. The present and substantial risk of imminent harm and loss of privacy have caused Plaintiff Donovan to suffer stress, fear, and anxiety.

142. Plaintiff Donovan has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Sydney Hollis

143. Plaintiff Sydney Hollis is a resident of Springfield, Illinois.

144. Plaintiff Hollis is employed by Defendant. As a condition of her employment, Plaintiff Hollis was required to provide Defendant with her full name, date of birth, address, bank account information, birth certificate, and Social Security number.

145. Plaintiff Hollis values her privacy and makes every effort to keep her personal information private.

146. Plaintiff Hollis only allowed Defendant to maintain, store, and use her Private Information because she believed Defendant would use basic security measures to protect her PII, such as requiring passwords and multi-factor authentication to access databases storing her Private Information.

147. In the instant that her PII was accessed and obtained by a third party without her consent or authorization, Plaintiff Hollis suffered injury from a loss of privacy.

148. Plaintiff Hollis has been further injured by the damages to and diminution in value

of her PII—a form of intangible property that Plaintiff Hollis entrusted to Defendant. This information has inherent value that Plaintiff Hollis was deprived of when her PII was placed on a publicly accessible database, exfiltrated by cybercriminals.

149. After the Data Breach occurred, Plaintiff Hollis experienced a significant increase in spam calls and phishing emails.

150. After the Data Breach occurred, Plaintiff Hollis received notifications from both Experian and Discover that her Personal Information has been found on the dark web.

151. The Data Breach has also caused Plaintiff Hollis to suffer imminent and impending injury arising from the present and substantially increased risk of future fraud, identity theft, and misuse resulting from her PII being placed in the hands of criminals.

152. As a result of the actual harm, Plaintiff Hollis has suffered the present and increased imminent risk of future harm, including lost time spent researching the data breach and monitoring her credit and bank accounts, which has, so far, expended several hours of her time including time spent freezing her credit.

153. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Hollis to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, reviewing financial statements, and monitoring potential fraudulent activities. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

154. The present and substantial risk of imminent harm and loss of privacy have caused Plaintiff Hollis to suffer stress, fear, and anxiety.

155. Plaintiff Hollis has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected,

and safeguarded from future breaches.

Plaintiff Robyn Campbell

156. Plaintiff Robyn Campbell is a resident of Greenville, Texas.

157. Plaintiff Campbell is a former employee of Defendant. As a condition of her employment, Plaintiff Campbell was required to provide Defendant with her full name, date of birth, address, bank account information, birth certificate, and Social Security number.

158. Plaintiff Campbell values her privacy and makes every effort to keep her personal information private.

159. Plaintiff Campbell only allowed Defendant to maintain, store, and use her Private Information because she believed Defendant would use basic security measures to protect her PII, such as requiring passwords and multi-factor authentication to access databases storing her Private Information.

160. In the instant that her PII was accessed and obtained by a third party without her consent or authorization, Plaintiff Campbell suffered injury from a loss of privacy.

161. Plaintiff Campbell has been further injured by the damages to and diminution in value of her PII—a form of intangible property that Plaintiff Baldwin entrusted to Defendant. This information has inherent value that Plaintiff Campbell was deprived of when her PII was placed on a publicly accessible database, exfiltrated by cybercriminals.

162. After the Data Breach occurred, Plaintiff Campbell has experienced a significant increase in spam calls and phishing emails.

163. After the Data Breach occurred, and as a result thereof, Plaintiff Campbell experienced fraud and identity theft in the form of unauthorized third parties logging into her Cash App and Pay Pal accounts.

164. Plaintiff Campbell had never previously had any issues or instances of financial fraud and only experienced such after, and, she believes, as a result of the Data Breach.

165. The Data Breach has also caused Plaintiff Campbell to suffer imminent and impending injury arising from the present and substantially increased risk of future fraud, identity theft, and misuse resulting from her PII being placed in the hands of criminals.

166. As a result of the actual harm, Plaintiff Campbell has suffered the present and increased imminent risk of future harm, including lost time spent researching the data breach and monitoring her credit and bank accounts.

167. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Campbell to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, reviewing financial statements, and monitoring potential fraudulent activities. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

168. The present and substantial risk of imminent harm and loss of privacy have caused Plaintiff Campbell to suffer stress, fear, and anxiety.

169. Plaintiff Campbell has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Amanda Pharr

170. Plaintiff Amanda Pharr is a resident of Fort Wayne, Indiana.

171. Plaintiff Pharr is a former employee of Defendant. As a condition of her employment, Plaintiff Pharr was required to provide Defendant with her full name, date of birth, address, bank account information, birth certificate, and Social Security number.

172. Plaintiff Pharr values her privacy and makes every effort to keep her personal information private.

173. Plaintiff Pharr only allowed Defendant to maintain, store, and use her Private Information because she believed Defendant would use basic security measures to protect her PII, such as requiring passwords and multi-factor authentication to access databases storing her Private Information.

174. In the instant that her PII was accessed and obtained by a third party without her consent or authorization, Plaintiff Pharr suffered injury from a loss of privacy.

175. Plaintiff Pharr has been further injured by the damages to and diminution in value of her PII—a form of intangible property that Plaintiff Pharr entrusted to Defendant. This information has inherent value that Plaintiff Pharr was deprived of when her PII was placed on a publicly accessible database, exfiltrated by cybercriminals.

176. After the Data Breach occurred, Plaintiff Pharr has experienced a significant increase in spam calls and phishing emails.

177. As a result of the Data Breach Plaintiff Pharr has experienced actual fraud and identity theft in the form of unauthorized third parties attempting to use her Personal Information to open credit card accounts, start cellular telephone services, and purchase a car.

178. The Data Breach has also caused Plaintiff Pharr to suffer imminent and impending injury arising from the present and substantially increased risk of future fraud, identity theft, and misuse resulting from her PII being placed in the hands of criminals.

179. As a result of the actual harm, Plaintiff Pharr has suffered the present and increased imminent risk of future harm, including lost time spent researching the data breach and monitoring her credit and bank accounts.

180. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Pharr to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, reviewing financial statements, and researching credit monitoring services and monitoring potential fraudulent activities. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

181. The present and substantial risk of imminent harm and loss of privacy have caused Plaintiff Pharr to suffer stress, fear, and anxiety.

182. Plaintiff Pharr has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Forrest Cooley

183. Plaintiff Forrest Cooley is a resident of Winchester, Kentucky.

184. Plaintiff Cooley is a former employee of Defendant. As a condition of his employment, Plaintiff Cooley was required to provide Defendant with his full name, date of birth, address, bank account information, birth certificate, and Social Security number.

185. Plaintiff Cooley values his privacy and makes every effort to keep his personal information private.

186. Plaintiff Cooley only allowed Defendant to maintain, store, and use his Private Information because he believed Defendant would use basic security measures to protect his PII, such as requiring passwords and multi-factor authentication to access databases storing his Private Information.

187. In the instant that his PII was accessed and obtained by a third party without his

consent or authorization, Plaintiff Cooley suffered injury from a loss of privacy.

188. Plaintiff Cooley has been further injured by the damages to and diminution in value of his PII—a form of intangible property that Plaintiff Cooley entrusted to Defendant. This information has inherent value that Plaintiff Cooley was deprived of when his PII was placed on a publicly accessible database, exfiltrated by cybercriminals.

189. After the Data Breach occurred, Plaintiff Cooley experienced a significant increase in spam calls and phishing emails.

190. Plaintiff Cooley has experienced fraud and identity theft as a result of the Data Breach including having his Social Security number used by an unauthorized third-party which resulted in it being "flagged". As a result, Plaintiff Cooley was denied a job he had applied for.

191. Plaintiff Cooley spent substantial time and effort correcting the situation, involving substantial travel, including three separate trips to the Social Security Administration's offices. Plaintiff Cooley was forced to get a new Social Security number as a result of the fraud he experienced due to the Data Breach.

192. Plaintiff Cooley believes that the fraud he experienced was due to the Data Breach because it occurred shortly after the Data Breach happened and because had never previously been involved in a data breach to his knowledge.

193. The Data Breach has also caused Plaintiff Cooley to suffer imminent and impending injury arising from the present and substantially increased risk of future fraud, identity theft, and misuse resulting from his PII being placed in the hands of criminals.

194. As a result of the actual harm, Plaintiff Cooley has suffered the present and increased imminent risk of future harm, including lost time spent researching the data breach and monitoring his credit and bank accounts.

195. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Cooley to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, reviewing financial statements, and monitoring potential fraudulent activities. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

196. The present and substantial risk of imminent harm and loss of privacy have caused Plaintiff Cooley to suffer stress, fear, and anxiety.

197. Plaintiff Cooley has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Taslima Aktar

198. Plaintiff Taslima Aktar is a resident of Fenton, Missouri.

199. Plaintiff Aktar is a former employee of Defendant. As a condition of her employment, Plaintiff Aktar was required to provide Defendant with her full name, date of birth, address, bank account information, birth certificate, and Social Security number.

200. Plaintiff Aktar values her privacy and makes every effort to keep her personal information private.

201. Plaintiff Aktar only allowed Defendant to maintain, store, and use her Private Information because she believed Defendant would use basic security measures to protect her PII, such as requiring passwords and multi-factor authentication to access databases storing her Private Information.

202. In the instant that her PII was accessed and obtained by a third party without her consent or authorization, Plaintiff Aktar suffered injury from a loss of privacy.

203. Plaintiff Aktar has been further injured by the damages to and diminution in value of her PII—a form of intangible property that Plaintiff Aktar entrusted to Defendant. This information has inherent value that Plaintiff Aktar was deprived of when her PII was placed on a publicly accessible database, exfiltrated by cybercriminals.

204. After the Data Breach occurred, Plaintiff Aktar has experienced a significant increase in spam calls and phishing emails.

205. The Data Breach has also caused Plaintiff Aktar to suffer imminent and impending injury arising from the present and substantially increased risk of future fraud, identity theft, and misuse resulting from her PII being placed in the hands of criminals.

206. As a result of the actual harm, Plaintiff Aktar has suffered the present and increased imminent risk of future harm, including lost time spent researching the data breach and monitoring her credit and bank accounts.

207. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Aktar to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, reviewing financial statements, and monitoring potential fraudulent activities. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

208. The present and substantial risk of imminent harm and loss of privacy have caused Plaintiff Aktar to suffer stress, fear, and anxiety.

209. Plaintiff Aktar has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

CHOICE OF LAW

210. Defendant is headquartered in Saint Louis, Missouri. That is the nerve center of Defendant's business activities—the place where high-level officers direct, control, and coordinate Defendant's activities, including data security, and where: (a) major policy; (b) advertising; (c) distribution; (d) accounts receivable departments; and (e) financial and legal decisions originate.

211. Data security assessments and other IT duties related to computer systems and data security occur at Defendant's Missouri headquarters. Furthermore, Defendant's response, and corporate decisions surrounding such response, to the Data Breach were made from and in Missouri. Finally, Defendant's breach of its duty to employees, current and former—including Plaintiffs and Class Members—emanated from Missouri.

212. It is appropriate to apply Missouri law to the claims against Defendant in this case due to Defendant's significant contacts with Missouri. Defendant is headquartered in Missouri; the relevant decisions, actions, and omissions were made in Missouri; and Defendant cannot claim to be surprised by the application of Missouri law to regulate its conduct emanating from Missouri.

213. To the extent Missouri law conflicts with the law of any other state that could apply to Plaintiffs' claims against Defendant, application of Missouri law would lead to the most predictable result, promote the maintenance of interstate order, simplify the judicial task, and advance the forum's governmental interest.

CLASS ACTION ALLEGATIONS

214. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs bring this action on behalf of themselves and the following proposed Nationwide Class, defined as follows:

> All persons residing in the United States who had their PII compromised as a result of the Data Breach that was publicly announced on June 13, 2024.

215. Plaintiff Weddle also brings this action on behalf of herself and the following proposed California Subclass (together with the Nationwide Class, hereafter referred to as the "Class"), defined as follows:

> All persons residing in California who had their PII compromised as a result of the Data Breach that was publicly announced on June 13, 2024.

216. Excluded from the proposed Classes are any officer or director of Defendant; any officer or director of any affiliate, parent, or subsidiary of Panera; anyone employed by counsel in this action; and any judge to whom this case is assigned, his or her spouse, and Members of the judge's staff.

217. **Numerosity.** Members of the proposed Class are likely to number in the tens of thousands and are thus too numerous to practically join in a single action. Membership in the Class is readily ascertainable from Defendant's own records.

218. **Commonality and Predominance.** Common questions of law and fact exist as to all proposed Class Members and predominate over questions affecting only individual Class Members. These common questions include:

a. Whether Defendant engaged in the wrongful conduct alleged herein,

b. Whether Defendant's inadequate data security measures were a cause of the data security breach,

c. Whether Defendant owed a legal duty to Plaintiffs and the other Class Members to exercise due care in collecting, storing, and safeguarding their PII,

d. Whether Defendant negligently or recklessly breached legal duties owed to

Plaintiffs and the other Class Members to exercise due care in collecting, storing, and safeguarding their PII,

e. Whether Plaintiffs and the Class are at an increased risk for identity theft because of the data security breach,

f. Whether Defendant failed to "implement and maintain reasonable security procedures and practices" for Plaintiffs' and Class Members' PII in violation of Section 5 of the FTC Act,

g. Whether Plaintiffs and the other Class Members are entitled to actual, statutory, or other forms of damages, and other monetary relief, and

h. Whether Plaintiffs and the other Class Members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

219. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs individually and on behalf of the other Class Members. Similar or identical statutory and common law violations, business practices, and injuries are involved.

Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous questions that dominate this action.

220. **Typicality:** Plaintiffs' claims are typical of the claims of the Members of the Class. All Class Members were subject to the Data Breach and had their PII accessed by and/or disclosed to unauthorized third parties. Defendant's misconduct impacted all Class Members in the same manner.

221. **Adequacy of Representation:** Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the other Class Members they

seek to represent; they have retained counsel competent and experienced in complex class action litigation, and Plaintiffs will prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

222. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiffs and the other Class Members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendant, making it impracticable for Class Members to individually seek redress for Defendant's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

COUNT I
NEGLIGENCE AND NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Class)

223. Plaintiffs restate and reallege paragraphs 1 through 222 above as if fully set forth herein.

224. Defendant requires its employees, including Plaintiffs and Class Members, to submit non-public PII as a condition of employment.

225. Defendant gathered and stored the PII of Plaintiffs and Class Members as part of its business, which affects commerce.

226. Plaintiffs and Class Members entrusted Defendant with their PII with the understanding that the information would be safeguarded.

227. By assuming the responsibility to collect and store this data, Defendant owed a duty to Plaintiffs and the Class to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiffs' and Class Members' PII from being compromised, lost, stolen, and accessed by unauthorized persons. This duty includes, among other things, designing, maintaining, and testing its data security systems to ensure that Plaintiffs' and Class Members' PII in Defendant's possession was adequately secured and protected.

228. Defendant owed a duty of care to Plaintiffs and Members of the Class to provide security, consistent with industry standards, to ensure that its systems and networks adequately protected the PII of its current and former employees.

229. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 (the "FTC Act"), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

230. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII.

231. Defendant owed a duty of care to Plaintiffs and Members of the Class because they were foreseeable and probable victims of any inadequate data security practices. Defendant knew or should have known of the inherent risks in collecting and storing the PII of its current and former employees and the critical importance of adequately securing such information.

232. Defendant's obligation to implement reasonable security measures also stems from the special relationship between Defendant and Plaintiffs and Class Members. This relationship was established because Defendant was entrusted with the confidential PII of Plaintiffs and Class Members as a necessary component of their employment.

233. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former employees' PII as it was no longer required to retain pursuant to the law and regulations.

234. Defendant knew, or should have known, of the risks inherent in collecting and storing PII and the importance of adequate security. Defendant knew about – or should have been aware of - numerous, well-publicized data breaches affecting businesses in the United States.

235. Moreover, Defendant had a duty to promptly and adequately notify Plaintiffs and Class Members of the Data Breach but failed to do so. It took Defendant approximately a month to detect the breach, followed by an additional two months to conduct an investigation. Even after concluding the investigation, Defendant delayed further by taking an additional month to finally notify Plaintiffs and Class Members.

236. Defendant had and continues to have duties to adequately disclose that Plaintiffs' and Class Members' PII within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by unauthorized third parties.

237. Defendant breached its duties, pursuant to the FTC Act and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Plaintiffs'

and Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to adequately monitor the security of its networks and systems;

c. Allowing unauthorized access to Class Members' PII;

d. Failing to detect in a timely manner that Class Members' PII had been compromised;

e. Failing to remove former employees' PII they were no longer required to retain pursuant to regulations; and

f. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that Class Members could take appropriate steps to mitigate the potential for identity theft and other damages.

238. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the damages that would result to Plaintiffs and Class Members.

239. Plaintiffs and Class Members were within the class of persons the provisions of the FTC Act were intended to protect and the type of harm that resulted from the Data Breach was the type of harm the statutes were intended to guard against.

240. Defendant's violation of Section 5 of the FTC Act constitutes negligence per se.

241. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

242. A breach of security, unauthorized access, and resulting injury to Plaintiffs and Class Members was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

243. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of corporate cyberattacks and data breaches.

244. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and Class Members could and would suffer if the PII were wrongfully disclosed.

245. Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing PII, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on its systems.

246. It was foreseeable that Defendant's failure to adequately safeguard PII would result in one or more types of injuries to Plaintiffs and Class Members.

247. Plaintiffs and Class Members had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

248. Defendant was in a position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

249. Defendant's duties extended to protecting Plaintiffs and Class Members from the

risk of foreseeable criminal conduct of third parties, which have been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. See Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

250. Defendant has admitted that the PII of Plaintiffs and Class Members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

251. But for Defendant's wrongful and negligent breaches of duties owed to Plaintiffs and Class Members, Plaintiffs' and Class Members' PII would not have been compromised.

252. There is a close causal connection between Defendant's failure to implement security measures to protect Plaintiffs' and Class Members' PII, and the harm, or risk of imminent harm, suffered by Plaintiffs' and the Class. PII was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care by adopting, implementing, and maintaining appropriate security measures.

253. As a direct and proximate result of Defendant's negligence, Plaintiffs' and Class Members have suffered and will suffer injury, including but not limited to: (i) the actual misuse of their compromised PII; (ii) invasion of privacy; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) an increase in spam calls, texts, and/or emails; and (vii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

254. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

255. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

256. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

257. Defendant's negligent conduct is ongoing, in that it still possesses Plaintiffs' and Class Members' PII in an unsafe and insecure manner.

258. Plaintiffs and Class Members are entitled to injunctive relief requiring Defendant to: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
BREACH OF IMPLIED CONTRACT AND BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING
(On behalf of Plaintiffs and the Class)

259. Plaintiffs restate and reallege paragraphs 1 through 222 above as if fully set forth herein.

260. Plaintiffs and Class Members were required to provide their PII to Defendant as a condition of receiving employment.

261. Plaintiffs and Class Members entrusted their PII to Defendant. In doing so, Plaintiffs and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and Class Members if their data had been breached and compromised or stolen, as well as an implied covenant by Defendant to protect Plaintiffs' PII in its possession.

262. In entering into the implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices would comply with relevant laws and regulations and align with industry standards.

263. Implicit in the agreement between Plaintiffs and Class Members and Defendant's obligation to: (a) take reasonable steps to safeguard that PII; (b) prevent unauthorized disclosure of the PII; (c) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII; (d) reasonably safeguard and protect the PII of Plaintiffs and Class Members from unauthorized disclosure or uses; and (e) retain or allow third parties to retain PII only under conditions that kept such information secure and confidential.

264. The mutual understanding and intent of Plaintiffs and Class Members, on the one hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing. Defendant required Plaintiffs and Class Members to provide their PII as a condition of employment. Plaintiffs and Class Members accepted the offers for employment and provided their PII.

///

///

265. In accepting the PII, Defendant understood and agreed that they were required to reasonably safeguard and otherwise ensure protection of the PII from unauthorized access or disclosure.

266. Plaintiffs and Class Member would not have entrusted their PII to Defendant in the absence of the implied contract between them and Defendant that Defendant would keep their PII reasonably secure.

267. Plaintiffs and Class Members would not have entrusted their PII to Defendant in the absence of their implied promise to monitor and ensure that the PII entrusted to it would remain protected by reasonable data security measures and remain confidential.

268. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant by providing their PII at Defendant's request.

269. Defendant breached the implied contracts made with Plaintiffs and the Class by failing to safeguard and protect their PII, by failing to delete the PII of Plaintiffs and the Class once the employment ended, and by failing to promptly provide accurate notice to them that their PII was compromised as a result of the Data Breach.

270. In addition, while Defendant had discretion in the specifics of how it met the applicable laws and industry standards, this discretion was governed by an implied covenant of good faith and fair dealing.

271. Defendant breached this implied covenant when it engaged in acts and/or omissions that are declared unfair trade practices by the FTC and state statutes and regulations. These acts and omissions included: omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Plaintiffs' and Class Members' PII; storing the PII of former employees, despite any valid purpose for the storage thereof having

ceased upon the termination of the business relationship with those individuals; and failing to disclose to Plaintiffs and Class Members at the time they provided their PII to it that Defendant's security systems failed to meet applicable legal and industry standards.

272. Defendant is liable for its breach of these implied covenants, whether or not it is found to have breached any specific express contractual term.

273. As a direct and proximate result of Defendant's breach of these implied contracts and implied covenants, Plaintiffs and Class Members sustained damages, as alleged herein, including the loss of the benefit of their bargain.

274. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

275. Plaintiffs and Class Members are entitled to injunctive relief requiring Defendant to enhance its data security measures. Specifically, this includes: (i) strengthening its data monitoring procedures; (ii) undergoing annual audits of those systems and procedures; and (iii) providing or continuing to provide comprehensive credit monitoring services to all Class Members for their lifetimes.

COUNT III
BREACH OF CONFIDENCE
(On behalf of Plaintiffs and the Class)

276. Plaintiffs restate and reallege paragraphs 1 through 222 above as if fully set forth herein.

277. At all times during Plaintiffs' and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiffs' and Class Members' PII that Plaintiffs and Class Members provided to Defendant.

278. Plaintiffs' and Class Members' PII constitutes confidential and unique

information. Indeed, Plaintiffs' and Class Members' Social Security numbers can be changed only with great difficulty and time spent, which still enables a threat actor to exploit that information during the interim.

279. As alleged herein and above, Defendant's relationship with Plaintiffs and Class Members was governed by terms and expectations that Plaintiffs' and Class Members' PII would be collected, stored, and protected in confidence, and would not be disclosed to any unauthorized third parties.

280. Plaintiffs and Class Members provided their respective PII to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PII to be disseminated to any unauthorized parties.

281. Defendant voluntarily received, in confidence, Plaintiffs' and Class Members' PII with the understanding that the PII would not be disclosed or disseminated to the public or any unauthorized third parties.

282. Due to Defendant's failure to protect Plaintiffs' and Class Members' PII, Plaintiffs' and Class Members' PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and Class Members' confidence, and without their express permission.

283. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiffs and Class Members have suffered damages as alleged herein.

284. But for the disclosure of Plaintiffs' and Class Members' PII, which is in violation of the parties' mutual understanding of confidence, Plaintiffs' and Class Members' PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. The Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class Members' PII, as well as the resulting damages.

285. The unauthorized disclosure of Plaintiffs' and Class Members' PII constitutes a violation of Plaintiffs' and Class Members' understanding that Defendant would safeguard and protect the confidential and unique PII.

286. The concrete injury and harm that Plaintiffs and Class Members suffered was the reasonably foreseeable result of Defendant's failure to ensure protection of the PII of Plaintiffs and Class Members.

287. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered or will suffer concrete injury, including, but not limited to: (a) actual identity theft; (b) the loss of the opportunity to determine how and when their PII is used; (c) the unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing of their PII; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, and repair the impact of the PII compromised as a direct and traceable result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

COUNT IV
INVASION OF PRIVACY
(On behalf of Plaintiffs and the Class)

288. Plaintiffs restate and reallege paragraphs 1 through 222 above as if fully set forth

herein.

289. Missouri established the right to privacy in Article 1, Section 15 of the Missouri Constitution.

290. Under Missouri law, the right of privacy is invaded when there is "(1) unreasonable intrusion upon the seclusion of another; or (2) appropriation of the other's name or likeness; or (3) unreasonable publicity given to the other's private life; or (4) publicity that unreasonably places the other in a false light before the public." *Sofka v. Thal*, 662 S.W.2d 502, 510 (Mo. banc 1983).

291. Plaintiffs and Class Members had a legitimate and reasonable expectation of privacy with respect to their PII and were accordingly entitled to the protection of this information against disclosure to and acquisition by unauthorized third parties.

292. Defendant owed a duty to its employees, including Plaintiffs and Class Members, to keep their PII confidential.

293. The unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing of PII, especially the type of information that is the subject of this action, is highly offensive to a reasonable person.

294. The intrusion was into a place or thing that was private and is entitled to be private.

295. Plaintiffs and Class Members disclosed their PII to Defendant as part of their employment with Defendant, but privately, with the intention that the PII would be kept confidential and protected from unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing. Plaintiffs and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

296. The Data Breach constitutes an unreasonable intrusion upon Plaintiffs' and Class Members' seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

297. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

298. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and Class Members.

299. As a proximate result of Defendant's acts and omissions, Plaintiffs' and Class Members' PII was accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by third parties without authorization, causing Plaintiffs and Class Members to suffer damages.

300. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that the PII maintained by Defendant can be accessed by, acquired by, appropriated by, disclosed

to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized persons.

301. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and Class Members. As such, Plaintiffs and the Class are entitled to damages in an amount to be proven at trial.

///

///

COUNT V
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

302. Plaintiffs restate and reallege paragraphs 1 through 222 above as if fully set forth herein.

303. Plaintiffs and Class Members conferred a monetary benefit on Defendant by providing it with their valuable PII.

304. Defendant knew that Plaintiffs and Class Members conferred a benefit upon it and accepted and retained that benefit by accepting and retaining the PII entrusted to it. Defendant profited from Plaintiffs' retained data and used Plaintiffs' and Class Members' PII for business purposes.

305. Defendant failed to secure Plaintiffs' and Class Members' PII and, therefore, did not fully compensate Plaintiffs or Class Members for the value that their PII provided.

306. Defendant acquired the PII through improper record retention practices, as it failed to disclose the previously alleged inadequate data security measures.

307. If Plaintiffs and Class Members had known Defendant would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their PII, they would not have agreed to the entrustment of their PII to Defendant.

308. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiffs and Class Members conferred upon it.

309. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) the actual misuse of their compromised PII; (ii) invasion of privacy; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the

Data Breach; (v) loss of benefit of the bargain; (vi) an increase in spam calls, texts, and/or emails; and (vii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

310. Plaintiffs and Class Members are entitled to restitution and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct, as well as return of their sensitive PII and/or confirmation that it is secure. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

311. Plaintiffs and Class Members may not have an adequate remedy at law against Defendant, and accordingly, Plaintiffs and Class Members plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT VI
BREACH OF FIDUCIARY DUTY
(On behalf of Plaintiffs and the Class)

312. Plaintiffs restate and reallege paragraphs 1 through 222 above as if fully set forth herein.

313. In light of their special relationship, Defendant has become the guardian of Plaintiffs' and Class Members' PII. Defendant became a fiduciary, created by its undertaking and guardianship of its employees' PII, to act primarily for the benefit of those employees, including Plaintiffs and Class Members. This duty included the obligation to safeguard Plaintiffs' and Class Members' PII and to timely notify them in the event of a data breach.

314. Defendant further breached its fiduciary duties owed to Plaintiffs and Class Members as former employees by failing to remove and otherwise destroy Plaintiffs' and Class Members' PII from Defendant's systems, as Defendant's employment relationship had ceased and Defendant no longer had any valid purpose for the maintenance and storage of that data.

315. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its relationship with them. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to properly encrypt and otherwise protect the integrity of the systems containing Plaintiffs' and Class Members' PII. Defendant further breached its fiduciary duties owed to Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach.

316. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to (a) actual identity theft; (b) the loss of the opportunity of how their PII is used; (c) the unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing of their PII; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII in its continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the

remainder of the lives of Plaintiffs and Class Members.

317. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses. As such, Plaintiffs and the Class are entitled to damages in an amount to be proven at trial.

COUNT VII
VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT
Cal. Civ. Code § 1798.100, *et seq.* ("CCPA")
(On behalf of Plaintiff Weddle and the California Subclass)

318. Plaintiff Weddle restates and realleges paragraphs 1 through 222 above as if fully set forth herein.

319. Plaintiff Weddle brings this Count on her own behalf and on behalf of the California Subclass (for purposes of this Count, the "Class").

320. The California Legislature has explained: "The unauthorized disclosure of personal information and the loss of privacy can have devastating effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm."[32]

321. The CCPA imposes an affirmative duty on businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected. Defendant failed to implement such procedures which resulted in the Data Breach.

322. It also requires "[a] business that discloses personal information about a

[32] *See* California Consumer Privacy Act (CCPA) Compliance, https://buyergenomics.com/ccpa-complience/ (last visited Jan. 14, 2025).

California resident pursuant to a contract with a nonaffiliated third party . . . [to] require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Cal. Civ. Code § 1798.81.5(c).

323. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

324. Plaintiff Weddle and Class Members are "consumer[s]" as defined by Civ. Code § 1798.140(g) because they are "natural person[s] who [are] California resident[s], as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017."

325. Defendant is a "business" as defined by Civ. Code § 1798.140(c) because Defendant:

a. is a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners";

b. "collects consumers' personal information, or on the behalf of which is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information";

c. does business in California; and

d. has annual gross revenues in excess of $25 million; annually buys, receives for the business' commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or derives 50 percent or more of its annual revenues from selling consumers' personal information.

326. The Private Information taken in the Data Breach is personal information as defined by Civil Code § 1798.81.5(d)(1)(A) because it contains Plaintiff Weddle's and Class Members' unencrypted first and last names, Social Security numbers, and financial account information among other information.

327. Plaintiff Weddle's and Class Members' unencrypted and unredacted Private Information was subject to unauthorized access and exfiltration, theft, or disclosure because their PII, including name, contact information, and Social Security numbers were wrongfully taken, accessed, and viewed by unauthorized third parties.

328. The Data Breach occurred as a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiff Weddle's and Class Members' PII. Defendant failed to implement reasonable security procedures to prevent an attack on its server or network, including its email system, by hackers and to prevent unauthorized access of Plaintiff Weddle's and Class Members' PII as a result of this attack.

329. More than 30 days prior to the filing of this Complaint, on or about June 19, 2024, Plaintiff Weddle provided Defendant with written notice of its violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). Defendant failed to respond and has not cured or is unable to cure the violations described therein. Plaintiff Weddle seeks all relief available under the CCPA including damages to be measured as the greater of actual damages or statutory damages in an amount up to seven hundred and fifty dollars ($750) per consumer per incident. *See* Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

330. As a result of Defendant's failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, in addition to actual or statutory damages, Plaintiff Weddle seeks injunctive relief, including public injunctive relief, declaratory relief, and any other relief as deemed appropriate by the Court.

COUNT VIII
DECLARATORY AND INJUNCTIVE RELIEF
(On Behalf of Plaintiffs and the Class)

331. Plaintiffs restate and reallege paragraphs 1 through 222 above as if fully set forth herein.

332. This Count is brought under the federal Declaratory Judgment Act, 28 U.S.C. § 2201.

333. As previously alleged, Plaintiffs and Class Members entered into an implied contract that required Defendant to provide adequate security for the PII it collected from Plaintiffs and Class Members.

334. Defendant owes a duty of care to Plaintiffs and Class Members to adequately secure their PII.

335. Defendant still possesses PII regarding Plaintiffs and Class Members.

336. Since the Data Breach, Defendant has announced minimal, if any, changes to its data security infrastructure, processes, or procedures aimed at addressing the vulnerabilities in its computer systems and security practices that allowed the breach to occur and to prevent future attacks.

337. Defendant has not satisfied its contractual obligations and legal duties to Plaintiffs and Class Members. In fact, now that Defendant's insufficient data security is known to hackers, the PII in Defendant's possession is even more vulnerable to cyberattack.

338. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiffs and Class Members. Further, Plaintiffs and Class Members are at risk of additional or further harm due to the exposure of their PII and Defendant's failure to address the security failings that lead to such exposure.

339. There is no reason to believe that Defendant's security measures have improved since the Data Breach to sufficiently meet its contractual obligations and legal duties.

340. Plaintiffs, therefore, seeks a declaration (1) that Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and

ordering Defendant to promptly correct any problems or issues detected by such

third-party security auditors,

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring,

c. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures,

d. Ordering that Defendant segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems,

e. Ordering that Defendant not transmit PII via unencrypted email,

f. Ordering that Defendant not store PII in email accounts,

g. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services,

h. Ordering that Defendant conduct regular computer system scanning and security checks,

i. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

j. Ordering Defendant to meaningfully educate its current, former, and prospective employees about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all other Members of the Class, respectfully requests the Court order relief and enter judgment in their favor and against

Defendant as follows:

A. For an Order certifying the Classes, and appointing Plaintiffs and their Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiffs and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Defendant to delete, destroy, and purge the PII of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendant to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiffs' and Class Members' respective lifetimes;

v. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;

vi. prohibiting Defendant from maintaining the PII of Plaintiffs and Class Members on a cloud-based database;

vii. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

viii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

ix. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

x. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

xi. requiring Defendant to conduct regular database scanning and securing checks;

xii. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees'

respective responsibilities with handling PII, as well as protecting the PII of Plaintiffs and Class Members;

xiii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiv. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xvi. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvii. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC

2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including, but not limited to, actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR A JURY TRIAL

Plaintiffs, on behalf of themselves and the proposed Classes, hereby demand a trial by jury as to all matters so triable.

Date: January 24, 2025

Respectfully Submitted,

*/s/ M. Anderson Berry*_____

M. Anderson Berry (*pro hac vice*)
Gregory Haroutunian (*pro hac vice*)
CLAYEO C. ARNOLD
A PROFESSIONAL CORPORATION
865 Howe Avenue
Sacramento, CA 95825
Telephone: 916.239.4778
Fax: 916.924.1829
aberry@justice4you.com
gharoutunian@justice4you.com

Ryan D. Maxey (*pro hac vice*)
MAXEY LAW FIRM, P.A.
107 N. 11th St. #402
Tampa, Florida 33602
Telephone: (813) 448-1125
ryan@maxeyfirm.com

Interim Co-Lead Class Counsel for Plaintiffs and the Proposed Classes

Raina C. Borrelli (*pro hac vice*)
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N. Michigan Avenue, Suite 1610
Chicago IL, 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
raina@straussborrelli.com

Laura Van Note, Esq. (*pro hac vice*)
COLE & VAN NOTE
555 12th Street, Suite 2100
Oakland, California 94607
Telephone: (510) 891-9800
Facsimile: (510) 891-7030
Email: lvn@colevannote.com

Jessica A. Wilkes (*pro hac vice*)
FEDERMAN & SHERWOOD
10205 North Pennsylvania Avenue
Oklahoma City, OK 73120
Telephone: (405) 235-1560
-and-
212 W. Spring Valley Road
Richardson, TX 75081
jaw@federmanlaw.com

Executive Committee for Plaintiffs and the Proposed Classes

CERTIFICATE OF SERVICE

I hereby certify that on January 24, 2025, a true and correct copy of the foregoing was electronically filed and served on all counsel of record using CM/ECF.

/s/ M. Anderson Berry
M. Anderson Berry